**Page 11**

***In a force-on-force exercise at Rocky Flats, mock "terrorists" were able to sneak into Rocky Flats by making a hole in a chain link fence. They were able to steal enough material to make several nuclear weapons and were only detected when they were exiting the facility.***

Although it is difficult to know precisely which force-on-force test the question references (since no date is included), it is assumed that it refers to one of the four performance tests conducted by OA in 1998, using the Navy SEALs as adversaries. Specifically, it is assumed that it refers to the second of the four tests, in which an adversary element successfully penetrated the target facility and then managed to evade contact with the protective force until the test was terminated. At the time of termination, the adversary was moving in the "buffer zone" that surrounds the site, and vehicle-mounted protective force patrols were attempting to cut off the exit of the adversary element.

It is not true that the adversary element entered the facility undetected; indeed, the adversaries were brought under fire shortly after their detection by alarm sensors on the inbound path. Instead, their use of speed, firepower, and concealment smoke enabled them to make a successful penetration, although the protective force neutralized several of the adversaries. The tests at Rocky Flats were the first major OA performance tests conducted after the mid-1990s suspension of testing and the first time that a DOE protective force had encountered an adversary element with the speed and tactical skill demonstrated by the SEALs. As a result of this test, the Rocky Flats protective force and other DOE protective forces began training to meet this higher standard of performance. Rocky Flats also acquired new equipment to deal with specific aspects of the scenario and to improve its response to perimeter alarms. Additionally, the consolidation of facilities at Rocky Flats since 1998 (part of the overall site closure process that is underway at that site) means that the situation at that site no longer resembles that which existed in 1998. This includes the number and variety of the vaults in use and their relationship to perimeter fencing and other security positions.

In planning the 1998 test under discussion, OA was not aware of any credible improvised nuclear device or comparable radiological dispersal threat associated with the facility in question. Therefore, the test scenarios all were based upon terrorist attempts to steal Special Nuclear Material.

*Page 12, question 1 (c): It is my understanding that it would only take as little as 1 minute for intruders to reach the vault where the special nuclear material is kept after they are first detected inside the outer fence of the facility. Is this true? If not, how long would it take?*

The protection measures in place provide sufficient detection and delay against intruders attempting to gain access to the vaults. The high level of system effectiveness is based on numerous enhancements implemented at the site since the 1998 exercise. As a result, intruders can not traverse the area in one minute. Examples of tasks that impede the speculated timeline include: traversing the area with added weight of explosives, tools, and weapons; protective force response and engagement; barrier breaching delays, etc.

The penetration methods available to the intruders, constrained by the design basis threat, determine the amount of time needed to gain access to the vault. Various penetration methods and times have been postulated and analyzed, and, where necessary, protection strategies have been deployed to mitigate the unacceptable risk associated with various scenarios. The times required to gain access to vault contents vary significantly, but all postulated scenarios exceed one minute.

*Page 12, question 1 (d): Have additional force-on-force exercises been conducted to ensure that the security upgrades are sufficient? If so, what were the results? If not, why not?*

Yes, force-on-force exercises have been successfully conducted and none reflected failures of the protection system. Any issues identified as needing improvement during such exercises are resolved through modifications to the system, including changes to procedures, protective force deployment, enhancement of equipment and barriers, etc.

*Page 12, question 2 (a): What steps were taken by Rocky Flats to ensure that this problem was corrected?*

The introductory paragraph to this question states, "This problem (inappropriate use of deadly force) had reportedly been identified in several force-on-force exercises at Rocky Flats from 1998-2000." This statement is based on information in a March 28, 2000 memorandum from Richard Levernier. All the quotes referenced from Mr. Levernier's memorandum are based on information he extracted from 1998 Rocky Flats performance test documentation. All exercises performed after 1998 have demonstrated an effective resolution of the lessons learned. Therefore, the referenced "problem" is over four years old. It's important to note that lessons learned are expected with the introduction of new and challenging exercise scenarios, as with the case in point. However, the site has continued to demonstrate the robustness of the overall protection program in precluding a threat of global proportions.

As a result of the 1998 exercises, Rocky Flats increased the scope of their protective force training program and supplemented the classroom training with field exercises. These steps greatly improved their comprehension and application of the Department's deadly force policy.

*Page 12, question 2 (b): Have additional force-on-force exercises been conducted to ensure that whatever measures taken by Rocky Flats to correct the problem actually did so? If so, what were the results? If not, how do you know that the steps taken are adequate?*

Numerous force-on-force exercises have been conducted since 1998. In each exercise since 1998, the protective force met the criteria for the use of deadly force.

*Page 12, question 2 (c): The memo stated that force-on-force exercises are judged to be successful even if there is inappropriate use of deadly force that results in fatalities of innocent people. Is this true?*

FOF exercises are one of many tools that the Department uses to evaluate its safeguards and security program. In addition, each tool measures a number of components of the protection system. Some of the components evaluated for FOF exercises include communication, individual tactics, team tactics, command and control, cover and concealment, deadly force, etc. The effectiveness of each of these components is based on multiple criteria. This methodology provides the Department with a mechanism for determining the effectiveness/success of each component independently, therefore serving as a continuous quality improvement process.

**SECTION: Force-on-Force Exercises at Rocky Flats, near Denver Colorado**

**Page 12, Question 2:** A March 28, 2000 memo from Richard Levernier, DOE Program Manager of Assessment and Integration to James L. Ford, Acting Director of Field Operations Division, stated that there had been "an alarming trend concerning the inappropriate use of deadly force" during force-on-force exercises at Rocky Flats. Apparently, according to documentation of these exercises, "the response of the protective force, when their orders to halt were disregarded, was to fire indiscriminately into the crowd of evacuees." The same document went on to state that "it is difficult to justify the wholesale killing of the building evacuees, when none among them - even the adversaries - had yet exhibited any behavior which offered a clear risk to either special nuclear material (SNM) or the life of any protective force member." This problem had reportedly been identified in several force-on-force exercises at Rocky Flats from 1998 - 2000.

**2d:** Don't you think there should be some penalty, such as a grade of "fail," for inappropriate use of deadly force during force-on-force exercises? If not, why not, since according to the memo, typical law enforcement training exercises consider inappropriate use of deadly force during training exercises to be a failure?

**Answer:** The goal of a Force-on-Force (FOF) exercise is to evaluate the capability of a given site's safeguards and security program to protect national security assets. The safeguards and security programs consist of many different elements, of which several can be partially evaluated by FOF exercises (i.e., ability to neutralize an adversary, communications, command and control, tactics, situational awareness, responsiveness, etc.). The information gathered from a FOF is used to determine the adequacy of a site's safeguards and security protection posture. Generally, the adequacy of a site's protection posture is based on whether or not SNM was protected as required (denial of access or prevention of removal from the site). If irregularities occur in the exercise (i.e., friendly fire, inappropriate use of deadly force, etc.) corrective actions, including refresher training on use of deadly force and tactical training are instituted.

**Page 12, Question 2e:** Has inappropriate use of deadly force been observed at other DOE sites during force-on-force exercises, and if so, where and under what circumstances? Is there a specific requirement to report cases where the guard force "kills" anyone other than the mock "terrorists"?

**Answer**: During Force-on-Force (FOF) exercises at the Savannah River Site 321-M facility (FY 1994), and Sandia National Laboratories – Albuquerque (FY 1998) inappropriate use of deadly force occurred. The 321-M exercise involved a mass exodus of individuals outfitted in MILES equipment from the given facility and the Protective Force mistakenly fired upon "civilians." The Sandia National Laboratory exercise involved a simulated hostage situation and during re-entry operations into the facility "civilians" were fired upon. As a result of these occurrences, corrective actions were instituted to include refresher training on deadly force and tactical awareness.

The inappropriate use of deadly force in a FOF exercise is detailed in the appropriate FOF exercise after-action report. There is not a specific requirement for a site to separately report incidents of inappropriate use of deadly force during FOF exercises.

**SECTION: Force-on-Force Exercises at Rocky Flats, near Denver Colorado**

**Page 13, Question 3:** A trip report for Rocky Flats March 21-26, 2000 and (sic) contained in Appendix C of the Project of Government Oversight report detailed a visit to Rocky Flats to observe force-on-force exercises and conduct additional security reviews.

**3a:** According to the report, DOE headquarters security personnel were initially denied access to the site, and were either denied information or were provided with it too late to be able to verify the results of the security exercises. Don't you agree that as a matter of policy, DOE personnel should have immediate access to the site as well as the materials necessary to make informed judgements about the adequacy of security? If so, what have you done to ensure that DOE contractors are aware of and comply with this policy? If not, why not?

**Answer:** DOE Headquarters personnel do have access to the Property Protection Areas (PPA) of a site based on the DOE standard badge. However, based on basic security practices, access to sensitive information and areas is predicated on clearly defined need-to-know, safety requirements and personnel security requirements. The need-to-know must be established with the cognizant site officials prior to the release of information or access to sensitive areas. The safety programs must be satisfied on a site-by-site basis to ensure the health and protection of the visitor and the employees. Direct hands-on access to material mandates that an individual be in a Personnel Security Assurance Program (PSAP) and have a specific need for access to that material, not for convenience. The measures listed above ensure the integrity of the safety and security of the materials and the employees.

**Page 13, Question 3b:** The trip report indicated that the visitors observed a truck entering a Protected Area of Rocky Flats without being searched. Is it DOE security policy to search all vehicles entering its facilities, especially Protected Areas, in light of the possibility that the detonation of a truck bomb close to radioactive material could disperse it over a large area, leading to widespread contamination and risk to public health and safety? If so, what have you done to ensure that this is now being done at Rocky Flats and other DOE facilities?

**Answer:** The current DOE protocol requires that all vehicles entering a Protected Area (PA) must have been searched for contraband. The increase in the Security Condition (SECON) levels at DOE facilities requires the appropriate searches to be conducted. Sites have visually observed the security operations to ensure that vehicles searches are being properly conducted.

In the instance referenced, the Rocky Flats Environmental Technology Site (RFETS) procedure is to either search or escort all vehicles entering the PA (some vehicles such as tankers can not be thoroughly searched, so they are under constant Protective Force escort to ensure they only go where they are supposed to go). The incident noted was in fact the fuel tanker which enters the PA for the purpose of fueling the Protective Force vehicles so they can remain inside the PA. The vehicle enters the PA and sets up a temporary fueling station and remains under constant Protective Force escort until all vehicles are fueled and the truck leaves the PA.

**Page 13, Question 3c:** The trip report also indicated that the Rocky Flats security personnel were not only told that explosives would be used in the force-on-force exercises, but were also told specific information about the size, shape and characteristics of the explosives. Do you believe that such an exercise provides useful, worst-case scenario information on the adequacy of the security forces, since real terrorists would certainly not provide such specific information in advance? If so, why? If not, what are you doing to ensure that security forces are not provided with too much advance information in the future?

**Answer:** Explosives used in Force on Force (FOF) exercises must be simulated, as we cannot use actual explosives at DOE facilities during FOF exercises. Typically a flash bang is used to simulate explosives. Due to the simulated nature of the explosives, it is necessary to brief the responders that the flash bang sound could represent different explosives/munitions (i.e., hand grenade, satchel charge, vehicle bomb, etc.) without explicitly stating what the sound will represent in the FOF exercise or where the explosives may be employed. This notification serves to alert FOF exercise participants that such a sound indicates the employment of explosives. During the exercise, the on-site controller notifies the appropriate FOF participants of an event and the consequences of the event (i.e., incapacitation, wall breach, etc.). If the FOF participants react solely to what they heard, rather than what the noise was simulating, the response would be incorrect. They are never told specifically where what types of explosive are being simulated, just the possible effects of the various explosives.

**Page 13, Question 3d:** The trip report also indicated that the "weapons" used to simulate gunfire were not working, that radio communications during the exercise were unreliable and intermittent, that the adversaries were not permitted to travel off roadways (a rule which no real terrorist would feel constrained to follow), that target buildings and the order of attacks were known to the security forces, and that the number of adversaries in the exercise was not representative of a "worst-case" scenario. Don't you think that these factors resulted in an exercise that did not even approach an approximation of a realistic threat? What are you doing to ensure that DOE headquarters security personnel are better able to participate in the planning and oversight of these exercises to ensure that they provide a more realistic assessment of security capabilities?

**Answer:** The factors listed are not completely accurate. Specifically, although there were limited issues with the performance of the multiple integrated laser engagement system (MILES) equipment, it applied to both the adversary and the protective force and the limitations were known to the adversary force in advance of the FOF exercise to develop alternative strategies. The radios provided for adversaries to use are the same radios used by the responding forces, but are set to different channels to which the Protective Force radios do not have access. Environmental rules prevent not only the adversaries, but also the responding forces from driving cross country except in actual emergencies. As such, when an adversary expressed the desire to go "cross country," the cone in the road was removed and the roadblock bypass simulated. There are only certain buildings which house SNM and these buildings are very well known to the Protective Force. In order to generate the most uncertainty for the Protective Force deployments, the exact building which will be the target for a particular exercise is never shared with the

Protective Force. The number of adversaries used meets the requirements of the DOE Design Basis Threat.

The artificialities inherent in DOE FOF simulations are well-known and documented, and subsequently minimized. Consequently, the DOE employees various means to maximize the safeguards and security information gathered from the FOFs while ensuring that the FOF exercises are as realistic as possible.

The DOE Headquarters Program Office personnel are involved in the planning and conduct of all Force on Force exercises at their respective sites. The Program Office personnel participate as controllers, observers and developers of the scenarios. The Office of Security provides technical assistance to the field sites and headquarters elements upon request.

*Page 14, Question 4(a): How long did it take DOE or DOE contractor security personnel to identify this employee?*

The August 2001 court testimony given by former DOE Special Assistant Peter Stockton in Civil Action 97-WM-2191 was reviewed and no reference can be found that correlates to the introductory paragraph preceding this question and the three subsequent questions. In addition, the site will need a specific reference to answer the question pertaining to a speculated security incident. No incident of the type speculated could be found correlating to the referenced date.

*Page 14, question 4 (b): The security investigation that revealed this problem took place in July 1999. When did Rocky Flats take steps to ensure that the plutonium was secured, and what steps were taken?*

Reference the response to question 4 (a).

*Page 14, question 4 (c): What has DOE done to ensure that the steps are effective and still in place? Have subsequent force-on-force exercises tested this particular vulnerability? If so, what was the result, and if not, why not?*

Reference the response to question 4 (a).

*Page 14, question 4 (d): Is there enough plutonium in this particular vault to construct an improvised nuclear device (i.e. homemade nuclear bomb) that would result in a detonation of nuclear yield?*

Reference the response to question 4 (a).

## FORCE-ON-FORCE EXERCISES
## FOR THE DOE TRANSPORTATION SECURITY DIVISION (TSD)

**PAGES 14-16**

**1) The TSD transports nuclear weapons and weapons-grade material from site to site within the DOE complex. According to a December 12, 1998, memo from Richard Levernier, DOE Program Manager of Assessment and Integration to Edward McCallum, then-DOE Director of the Office of Safeguards and Security, the TSD failed six out of seven force-on-force simulations in December 1998.**

**a) What corrective measures have been taken to ensure that security associated with the transportation of weapons-grade material was improved?**

**Answer:** The Office of Transportation Safeguards (OTS) utilizes a formal evaluation process to assess the security posture of the Transportation Safeguards System (TSS). Security issues are identified, addressed and enhancements are implemented as appropriate. Every opportunity to enhance technology and protective force capability is carefully weighed against current operating conditions, Departmental requirements and postulated threats. This iterative evaluation process is part of the overall OTS management system. Specific details regarding enhancements are classified.

Recapture and recovery became the overall issue facing OTS. OTS developed a two-phased "Get Well Plan" with Phase One including immediate enhancements for recapture and recovery. Enhancements were briefed to headquarters officials such as the Under Secretary, the Director of Counter Intelligence, the Chief Information Officer, the Director of OSS as well as Defense Programs management during the April – June 1999 time frame. These actions were implemented by December 1999, and additional enhancements have been and are continuing to be made.

**b) Have additional force-on-force exercises been conducted on the TSD to ensure that the corrective security measures are effective? If so, when, and what were the results? If not, why not, and how do you know that shipments of these materials are safe from attack?**

**Answer:** Force-on-Force (FOF) exercises are a critical component of OTS's formal evaluation process. FOF are conducted regularly for both training and validation purposes. FOF exercises have been conducted in 2000, 2001 and 2002. FOF validation exercises conducted in 1999, 2000, 2001 and 2002 indicate that OTS is operating at low risk. Specific results of FOF exercises are classified.

Following the events of September 11, 2001, all weapons convoys were in safe havens within a short period of time. The NNSA then undertook a comprehensive review of security across the complex and implemented revised/additional security measures and practices.

**c) Do you agree that in the event of a real (and successful, as 6 out of 7 of these mock attacks were) attack on a shipment of weapons-grade material, a suicidal and knowledgeable group of terrorists could quickly assemble and detonate an improvised nuclear device (i.e. a homemade nuclear bomb) or a radiological dispersion device (i.e. a dirty bomb)? If not, why not?**

**Answer:** The Department has extensive protection measures in place to mitigate against the remote possibility that a terrorist organization could construct or detonate a device.

**d) Are shipments of nuclear weapons and weapons-grade materials expected to be secure against armor piercing incendiary rounds? If not, why not, since a June 1999 General Accounting Office report entitled "Weaponry: Availability of Military .50 Caliber Ammunition" concluded that more than 100,000 rounds of Pentagon-surplus armor-piercing incendiary rounds have been sold on the civilian market?**

**Answer:** The OTS has completed an extensive evaluation of the .50 caliber armor-piercing round. Post September 11, 2001, the OTS implemented significant classified changes to the Transportation Safeguards System that will also have a mitigating effect on .50 caliber weapons used against the TSS. During Fiscal Year 2000, the Office of Technology Development and OSS, initiated plans to review the effect of API (50 cal) on a wide range of DOE assets.

**e) Are shipments of high-level nuclear waste undertaken with the same levels of security as shipments of nuclear weapons or weapons-grade materials? If not, why not, since these material are highly radioactive and could also be used to construct and detonate radiological dispersion devices? Please also fully describe all differences in the security measures taken for these different types of shipments.**

**Answer:** Specific Nuclear Materials Shipments are part of the OTS mission and are conducted with high levels of security.

**f) Have force-on-force exercises been conducted on shipments of high level nuclear waste? If so, what were the results? If not, why not, since these materials are highly radioactive and could also be used to construct and detonate radiological dispersion devices?**

**Answer:** FOFs of Special Nuclear Material shipments are included in the overall evaluation process to assess the security posture of the TSD. FOF validation exercises conducted in 1999, 2000, and 2001, indicate that OTS is operating at low risk.

**c) Do you agree that in the event of a real (and successful, as 6 out of 7 of these mock attacks were) attack on a shipment of weapons-grade material, a suicidal and knowledgeable group of terrorists could quickly assemble and detonate an improvised nuclear device (i.e. a homemade nuclear bomb) or a radiological dispersion device (i.e. a dirty bomb)? If not, why not?**

**Answer:** The Department has extensive protection measures in place to mitigate against the remote possibility that a terrorist organization could construct or detonate a device. The way we store, handle and transport nuclear weapons and other strategic materials results in the most highly protected assets in this nation. There are no places that a terrorist could attack with any real expectation of success.

**d) Are shipments of nuclear weapons and weapons-grade materials expected to be secure against armor piercing incendiary rounds? If not, why not, since a June 1999 General Accounting Office report entitled "Weaponry: Availability of Military .50 Caliber Ammunition" concluded that more than 100,000 rounds of Pentagon-surplus armor-piercing incendiary rounds have been sold on the civilian market?**

**Answer:** The OTS has completed an extensive evaluation of the .50 caliber armor-piercing round. Post September 11, 2001, the OTS implemented significant classified changes to the Transportation Safeguards System that will also have a mitigating effect on .50 caliber weapons used against the TSS. During Fiscal Year 2000, the Office of Technology Development and OSS, initiated plans to review the effect of API (50 cal) on a wide range of DOE assets.

**e) Are shipments of high-level nuclear waste undertaken with the same levels of security as shipments of nuclear weapons or weapons-grade materials? If not, why not, since these material are highly radioactive and could also be used to construct and detonate radiological dispersion devices? Please also fully describe all differences in the security measures taken for these different types of shipments.**

**Answer:** Specific Nuclear Materials Shipments are part of the OTS mission and are conducted with high levels of security.

**f) Have force-on-force exercises been conducted on shipments of high level nuclear waste? If so, what were the results? If not, why not, since these materials are highly radioactive and could also be used to construct and detonate radiological dispersion devices?**

**Answer:** FOFs of Special Nuclear Material shipments are included in the overall evaluation process to assess the security posture of the TSD. FOF validation exercises conducted in 1999, 2000, and 2001, indicate that OTS is operating at low risk.

**2) An April 19, 1999, memo from Richard Levernier, DOE Program manager of Assessment and Integration to Edward McCallum, then-DOE Director of the Office of Safeguards and Security, stated that although TSD had received copies of several security reports designed to improve security of nuclear weapons materials shipments, that TSD had yet to provide comments as requested (comments had been requested from TSD on 2 of the reports more than 2 months earlier). A later August 1999 briefing for General Habiger, then DOE's "security czar," indicated that TSD did not propose any compensatory measures in response to the failed exercises, and that TSD wanted to defer all outstanding security issues until 2000. The briefing also recommended that TSD not be given a grade of "satisfactory" or "green" in the 1999 report on DOE Security to the President until it took compensatory security measures.**

**a) When did TSD finally respond with its comments on the security reports? Why did it take so long, given the importance of ensuring the security of nuclear weapons and weapons-grade material? Please identify the individual(s) responsible for providing comments on these reports. What performance ratings or performance evaluations did such individual(s) receive for work performed during this period?**

**Answer:** Interactions between OTS, Defense Programs and OSS were ongoing beginning in January 1999. Formal briefings regarding OTS security were presented to headquarters officials such as the Department's Under Secretaries, the Director of Counter Intelligence, the Chief Information Officer, the Director of OSS as well as Defense Programs management during the April – June 1999 timeframe. In August 1999 a matrix of completed, on-going and planned activities was submitted to OSS. An updated matrix, closing issues, was submitted in December 1999. There are no open issues.

Additionally, the DOE Office of Inspector General conducted a review of the DOE SSSP process, and OTS was included in this review. In November 2000, OTS formally responded to the DOE Inspector General recommendations. Recommendations have been implemented.

**b) When were compensatory security measures taken by TSD in response to the December 1998 force-on-force simulations that resulted in 6 out of 7 failures? Whey did it take so long, given the importance of ensuring the security of nuclear weapons and weapons-grade material? If no measures have been taken, why not, especially in light of the events of September 11?**

**Answer:** OTS utilizes a formal evaluation process to assess the security posture of the TSD. As issues are identified they are addressed. Enhancements are implemented as appropriate. Every opportunity to enhance technology and protective force capabilities is carefully weighed against current operating conditions, Departmental requirements and postulated threats. This iterative evaluation process is part of the overall OTS management system. Some enhancements were made in December 1998. Recapture enhancements were implemented by December 1999.

Following the events of September 11, 2001, all weapons convoys were in safe havens within 90 minutes. The NNSA then undertook a comprehensive review of security across the complex and implemented revised/additional security measures and practices.

**c) Please provide a copy of the 1999 DOE Report to the President on Safeguards and Security. What grade did TSD get? If a grade of "satisfactory" or "green" was given, was that because TSD took the required compensatory steps to address flaws in security? If not, then how was such a grade justified?**

**Answer:** The 1999 DOE Report to the President on Safeguards and Security is classified. OTS received a "green" rating. Ratings are based on external surveys and reports.

**d) Please provide a copy of the 2000 DOE Report to the President on Safeguards and Security. What grade did TSD get? If a grade of "satisfactory" or "green" was given, was that because TSD took the required compensatory steps to address flaws in security? If not, then how was such a grade justified?**

**Answer:** The 2000/2001 NNSA Report to the President on Safeguards and Security has not yet been issued. For Calendar Years 2000/2001, information has been combined in one report. These two years were consolidated due to the significant transition which began in CY 2000 as a result of the establishment of the NNSA. The report, when issued will be classified.

**e) In general, do you believe that weaknesses in security should be addressed and corrected immediately upon their discovery? If not, why not? Do you believe that it is acceptable to defer their correction for an extended period of time after their discovery? If so, why, especially in light of the events of September 11?**

**Answer:** Security issues are addressed in a timely manner and must be evaluated against sound decision criteria.

Following the events of September 11, 2001, the security posture was raised throughout the weapons complex, enhanced protection measures were employed, and all weapons convoys were in safe haven within 90 minutes. The NNSA then undertook a comprehensive review of security across the complex and implemented revised/additional security measures and practices.

**3) In early 1999, a special force-on-force test on the TSD was run at Fort Hood for high-level DOE HQ personnel. The TSD forces were successful in repelling an attack from the U.S. Army Special Forces mock "terrorists." However, one of the Special Forces members reportedly discovered that the TSD forces had acquired a paper copy of the mock "terrorists" plan for the exercise, and had used it to cheat.**

**a) Please provide copies of all reports, email and correspondence concerning this incident.**

**Answer:** OTS conducted a Joint Training Exercise with the State of Texas law enforcement and emergency management, Ft. Hood military and other organizations. Senior officials of all participating organizations are invited to attend a "VIP Day" and DOE HQ personnel often attend the JTX.

The NNSA has no documents related to this incident. On the two occasions when the Special Forces member made this statement to OTS management, he would not provide any specific details. The Exercise Director asked the Special Forces member specifically who was cheating and the Special Forces member refused to provide the information. The Exercise Director advised the Special Forces member it would be difficult to follow through without identifying the individual accused of cheating. The Exercise Director held a meeting with all execise controllers including the Opposition Force Lead Controller and conducted an informal inquiry. None of the controllers including the Opposition Force Lead Controller had observed nor were they aware of any individual having used a paper copy of the mock "terrorist" attack to cheat during the exercise.

**b) What actions have you taken to identify and discipline whoever was responsible for deciding to cheat on the exercises? If no actions have been taken, why not?**

**Answer**: OTS was unable to take actions because the Special Forces member would not provide any specific details.

**c) Has this exercise been repeated? If not, why not, and how can we be assured that any shipments of nuclear weapons or weapons-grade material is safe?**

**Answer:** Force-on-Force (FOF) exercises are a critical component of OTS's formal evaluation process. FOF are conducted regularly for both training and validation purposes. FOF exercises have been conducted in 1999, 2000, 2001 and 2002. These validation exercises indicate that OTS is operating at low risk. Specific results of FOF exercises are classified.

**4) September 2000 report by the DOE Inspector General made numerous recommendations related to improving security at TSD. Have each of these recommendations been recorded in the Safeguards and Security Information Management System? If not, why not? Have each of the recommendations been implemented? If not, why not?**

**Answer:** Safeguards and Security Information Management System (SSIMS) data management is managed by the DOE office of Safeguards Security, thus the DOE Office of Safeguards and Security determines what issues are/are not entered into SSIMS. The DOE Office of Inspector General conducted a review of the DOE SSSP process, and OTS was review. In November 2000, OTS formally responded to the DOE Inspector General recommendations. Recommendations have been implemented.

**5) How many shipments of special nuclear material have been made since January 1999?**

574 Shipments

**SECTION: Questions on the Design Basis Threat (DBT) for DOE Facilities**

The DBT is the set of regulations, developed in consultation with intelligence agencies, that describe the threat against which DOE facilities need to be protected. The unclassified version of the December 1998 DOE DBT states that "DOE interests shall be protected against activities which include unauthorized access; theft, diversion or loss of control of nuclear weapons; weapons components, special nuclear material, associated technologies and hardware and critical technologies; sabotage; espionage; loss or theft of classified matter or Government property; and other acts which may cause unacceptable adverse impacts on national security, the health and safely of employees, the public or the environment." Each DOE site is required to develop an annual Site Safeguards and Security Plan (SSSP) which describes how it would protect against the DBT. The SSSP is developed by the DOE contractors who run the site and must then be analyzed and approved by DOE.

**Page 17, Question 1**: Will the DBT for DOE facilities be changed, in light of the events of September 11? If not, why not? If so, when will the changes be completed?

**Answer**: Based on the events of September 11, 2001, the DOE, in cooperation with the Department of Defense (DOD), recognized that a revised interim threat statement must be developed. Consequently, the DOE and DOD have developed a draft "Interim Joint Threat Policy Statement" (IJTPS) which specifically addresses the events of September 11, 2001. The IJTPS is in review and comment in the DOE and DOD as of May 2002. It is anticipated that the IJTPS will be finalized during the Summer 2002. The formal DOE DBT is derived from the Postulated Threat developed by the U.S. intelligence community. The Postulated Threat data-gathering phase, which considers the events of September 11, 2001, is in process. The first draft of the Postulated Threat is scheduled for late Spring 2002. The final Postulated Threat is scheduled for release in the Fall 2002. The DOE DBT began in May 2002. The official DOE DBT is scheduled to be issued within 90 days of the official Postulated Threat.

**Page 17, Question 2**: If the DBT will be changed, when will the DOE sites be required to submit their new SSSPs for analysis and approval? How long will it take before the new security plans are approved and implemented?

**Answer**: By DOE Order 470.1, those facilities required to prepare and submit Site Safeguards and Security Plans (SSSPs), must review and make necessary corrections to the SSSPs on an annual basis. The DOE sites will therefore have up to one year from the time of DBT issuance to submit the SSSPs to the appropriate Program Office. The Program Offices have 60 days to review, comment and concur. The implementation period of the SSSP will vary. Part of the SSSP outlines the risk to a facility, the safeguards and security measures required to mitigate unacceptable risks and a time-table for the implementation of those measures.

**Page 17, Question 3**: Will force-on-force exercises be conducted at each facility to test the adequacy of the new SSSPs? When will they be completed?

**Answer**: DOE Order 470.1, Chapter III, and DOE Manual 473.2-2, Chapter VII, require each site to conduct force-on-force (FOF) exercises to validate and performance test the worst case scenarios as postulated by vulnerability analyses. The information generated by the FOFs is used in the vulnerability assessment process to support the SSSP. The FOFs must be completed prior to the approval of the SSSP.

**Page 18, Question 8**: Have force-on-force exercises been conducted at all sensitive DOE facilities to ensure that they are capable of repelling attacks using chemical and biological weapons? If not, why not, and how do you know that DOE facilities are in compliance with the 1995 and 1996 Presidential Decision Directives?

**Answer**: Force-on-Force exercises have been conducted considering the employment of chemical and biological weapons. The exercises have required the donning of the protective masks and operating communications and weapons and other gear with the mask on.

The Office of Security implemented a program called the Chemical Defense Assessment Team (CDAT) in Fiscal Year 2000. The CDAT conducts vulnerability assessments of critical DOE facilities to determine the susceptibility of the facility to chemical attacks.

**Page 18, Question 9**: What will the new post-9/11 Design Basis Threat require in terms of increased numbers of guard forces at each DOE site that contains special nuclear material? What about purchasing new guard force weapon systems?

**Answer**: The number and capabilities of the adversaries in the forthcoming DBT are unknown at this time. The revised Postulated Threat and associated DBT are not scheduled for publication until the Fall 2002. It is not possible to estimate the numbers of protective force members and associated equipment required based on the forthcoming DBT at this time.

**Page 18, Question 10**: How will DOE ensure that the size of the guard force, weapons systems used by the guard force, and tactics used by the guards force are adequate to deny attackers access to the DOE facilities?

**Answer**: The DOE has an established risk management process embodied in the SSSP program. The SSSP vulnerability assessment process utilizes computer modeling, computer-based engagement simulations, expert judgment, performance testing and force-on-force exercises to accurately assess the safeguards and security protection posture. These tools and programs ensure that the appropriate levels of protection are afforded to DOE assets.

**SECTION: Question on Critical Systems Flaws in DOE Safeguards and Security**

**Page 18, Question 1**: An August 30, 1999 memo from Barbara R. Stone of DOE's Office of Safeguards and Security Evaluations to General Eugene Habiger, then Director of DOE's Office of Security and Emergency Operations lists numerous critical systems flaws in DOE safeguards and security. For each of the following failures identified in the memo, please describe whether the problems were entered into the Safeguards and Security Information Management System, whether the required corrective action plans were prepared within 30 days, and what steps have been taken to resolve the problems:

**Answer**: The opinioned critical system flaws in DOE safeguards and security identified in the August 30, 1999, memo from Barbara R. Stone to General Eugene Habiger were not entered into the Safeguards and Security Information Management System (SSIMS). The SSIMS was designed and developed to track deficiencies identified in surveys and inspections conducted by DOE Field Offices, Office of Security Evaluations, Inspector General and General Accounting Office. The policy and procedures for reporting and tracking survey findings and corrective actions are contained in DOE Order 470.1 Safeguards and Security Program, and following policy memoranda: "Reporting and Tracking of Survey Findings and Corrective Actions" dated March 28, 1995, and "Tracking of Deficiencies Identified in the Office of Security Evaluation Inspection Reports" dated August 24, 1999. As such, the memo in question did not meet the criteria for inclusion in SSIMS.

**Page 18, Question 1a:** The failure to properly characterize DOE facility security features (such as doors, barriers, alarm systems, etc.) within the ASSESS database;

**Answer**: The ASSESS database contains default starting values for the most common security features. The vulnerability analyses process requires that critical protection features be performance tested and expert judgment be applied to ascertain the actual performance parameters rather than sole reliance on the default values. The Office of Security instituted a project in 1998 to update the ASSESS databases as new performance data became available. Additionally, the Office of Security has continuously provided national laboratory expertise and reports to field sites to assist in the accurate characterization of security equipment performance.

**Page 18, Question 1b:** The failure to update DOE facility security features within the ASSESS database features (such as doors, barriers, alarm systems, etc.) when these features are upgraded;

**Answer**: The ASSESS database contains default starting values for the most common security features. The vulnerability analyses process requires that critical protection features be performance tested and expert judgment be applied to ascertain the actual performance parameters rather than sole reliance on the default values. Additionally, the Office of Security instituted a project in 2000 to update the ASSESS databases as new performance data became available.

**Page 18, Question 1c:** The failure to utilize the ASSESS database calculations of the likely types of insider threats;

**Answer**: The DOE determined that the ASSESS insider module is limited in the type of insiders included and the calculations that can be performed. The DOE requires an in-depth insider analysis to be performed at each facility utilizing other vulnerability analysis tools suited to the task. The next generation vulnerability analysis tool, Adversary Time-Line Analysis System (ATLAS), currently in development is being designed to incorporate a more comprehensive insider modeling tool suite.

**Page 18, Question 1d:** The failure to correct errors in the combat simulation model used to model tactical engagements at DOE facilities;

**Answer**: The Office of Security acknowledged weaknesses in the combat simulation modeling databases in the summer of 1999. The Office of Security developed a baseline weapons effects and capabilities database that all users would be required to use for validation purposes. The database was transmitted to the necessary DOE sites in October 1999.

**Page 18, Question 1e:** The failure to include a full range of possible adversary weapons in either the combat simulation model or the actual force-on-force exercises conducted at DOE facilities;

**Answer**: The combat simulation models and the force-on-force exercises are limited by the design of the software and MILES equipment, respectively. In order to ensure that the adversaries are given the full range of capabilities denoted in the DBT and the Adversary Capabilities List, the Department utilizes experts in the application of the combat simulation tools and force-on-force exercises to make "controller" calls to simulate any capability that it is not possible to model. DOE continues to research and test alternative methods for combat simulation modeling and force-on-force exercises to ensure the most accurate portrayal of the safeguards and security protection posture at a DOE site.

**Page 18, Question 1f:** The failure to adequately model tactics likely to be used by the mock "terrorists;"

**Answer**: The tactics employed by the mock "terrorists" are designed to give the adversary the most advantage. The tactics are developed by personnel skilled in small unit tactics from the DOE and support from other agencies. The models depict, as accurately as possible given the model limitations, the tactics most advantageous to the adversary. In the event the model cannot accurately portray the preferred tactics, administrative measures are employed to achieve the equivalent advantage for the adversary forces.

**Page 18, Question 1g:** The failure to properly account for the element of surprise likely to be associated with a real terrorist attack in the combat simulation models in order to determine ways (i.e. new training, tactics, or weapons for the guard force) in which to compensate for it.

**Answer**: The element of surprise is incorporated into the models. This factor is normally represented in increased response time delays for the site protection force and by allowing the adversary forces to proceed on the attack pathway unchallenged for a set period of time. The

sites do utilize the models to simulate variations in the attack scenarios to develop, test and verify the proper response plans.

Answer to question one regarding "Questions on DOE Retaliation Against Whistleblowers" starting on page 19 (bottom) of the January 23, 2002 letter from Congressman Markey.

**Question**: a) How many formal or informal complaints of reprisals or retaliation have been made by DOE or DOE contractor/subcontractor employees who expressed security concerns since the memo was written [in June 1999]?

**Answer**: a) A survey of DOE's Employee Concerns Program Offices in the field indicates that no informal complaints of reprisal have been made since June 1999. Formal complaints may be filed with the DOE, the Department of Labor, or under state law. We are aware of four formal complaints that have been filed since June 1999; two were filed with DOE, one with the U.S. Department of Labor, and one under California state law.

**Question**: b) For each of these cases, please describe the circumstances, and how the complaint was resolved.

**Answer**: 1) Pursuant to its Contractor Employee Protection Program codified at 10 CFR Part 708, the DOE has received two formal complaints filed by Mr. Jimmie L. Russell and Mr. Ronald E. Timm.

Jimmie L. Russell filed a complaint of retaliation on October 12, 1999 against the University of California, managing contractor for the Los Alamos National Laboratory. Russell was an employee of Comforce and was working as a subcontractor to the Los Alamos National Laboratory. Russell was a certified security auditor with extensive military, academic and law enforcement experience. He was providing staffing services to the Los Alamos National Laboratory Security Division's Plans and Assessment Office. Russell was responsible for conducting audits and assessments of Safeguards and Security programs and preparing written reports of his findings. These reports communicated the assessors' findings of security, safety and management deficiencies on a regular basis. Russell made disclosures concerning management issues, breaches in security procedures and safety violations at the Los Alamos National Laboratory. He alleged that certain University of California employees retaliated against him and that the retaliation resulted in the termination of his work at the Los Alamos National Laboratory. DOE investigated the complaint, and a Hearing Officer at the DOE's Office of Hearings and Appeals ruled in favor of the Mr. Russell. The Hearing Officer's Decision is available on the OHA web site and is published at http://www.oha.energy.gov/cases/whistle/vbh0017.htm. The contractor filed an appeal, but it was withdrawn when the parties executed a settlement.

Ronald E. Timm, the president of RETA Security, filed a complaint of retaliation on August 31, 2001 against DOE's Office of Safeguards and Security. RETA Security was a subcontractor to SAIC who was a prime contractor with DOE. RETA Security was responsible for identifying significant security issues at six DOE sites. For each site reviewed, the findings were documented in official, classified reports. The reports were circulated to DOE management to inform them of the analysis results. Allegedly, DOE's

Office of Safeguards and Security began efforts to shift RETA Security's work from analysis of current DOE security programs to security-related study development. RETA Security alleged that because its findings outlined serious concerns about security at DOE sites, removing RETA Security from the process would make it easier for those seeking to hide these concerns. Eventually a "Stop Work" order was issued ending all work by RETA Security. RETA Security viewed this order as clear evidence of retaliation by DOE's Office of Safeguards and Security and filed a complaint with the DOE/NNSA Albuquerque Operations Employee Concerns Program Office. After reviewing the circumstances, that Office dismissed the complaint for lack of jurisdiction. Mr. Timm appealed that dismissal to the DOE's Office of Hearings and Appeals (OHA). OHA affirmed the dismissal of the complaint because the DOE contractor employee whistleblower protection program does not cover complaints such as Mr. Timm's where the alleged wrongdoer is the DOE and not a contractor. The decision on appeal is published at http://www.oha.energy.gov/cases/whistle/vbu0077.htm. Mr. Timm has requested that the Secretary of Energy review the appellate decision. That request is pending.

2) On January 14, 2002, two former guards filed a complaint with the U.S. Department of Labor pursuant to 42 USC 5851 in which they allege retaliation by the University of California. The matter is pending.

3) On the same day, a complaint was filed by both individuals with LLNL under California Government Code 8547.10, which allows University of California (UC) employees to file claims with UC alleging retaliation, reprisal, etc. concerning protected disclosures. Under LLNL's internal implementing procedures, a Retaliation Complaint Officer (RCO) has been appointed by LLNL to review and investigate the complaint. The RCO's report should be completed in April, 2002 and will then be forwarded to the Director of LLNL for his decision concerning the complaint. Complainants can appeal LLNL's decision to higher UC authority or can file a subsequent action in State court.

**SECTION: Questions on Resources Allocated to and Organization of DOE Safeguards and Security**

**Page 20, Question 1:** June 8, 1999 Congressional testimony given by Edward J. McCallum, then-Director of the DOE Office of Safeguards and Security, stated that "since 1992, the number of protective forces at DOE sites nationwide has decreased by almost 40%....while the inventory of nuclear material has increased by more than 30%." Numerous critics of DOE security have observed that the budget for security often completes directly with other mission activities such as nuclear weapons research.

**1a:** For each year since 1992, and for each DOE site, please list the numbers and levels of training (i.e. Special Response Team, etc.) of the protective force personnel employed on the site.

**Answer:** The Department has several levels of protective force personnel. See attached documents which define the levels and training requirements of protective force personnel, statistics on the numbers of protective personnel employed from FY 1992 through FY 2001, and a graphic representation of DOE-wide protective force strength.

Please note that the on-board staff level is not the best measure of protective force security provided since the levels varied through the fiscal year and do not capture overtime worked. Future data calls will request information about protective force overtime.

## Contractor Protective Force Officer Category Definitions

### Uniformed Officers

Security Officer (SO): An unarmed individual assigned the responsibility to accompany persons who lack need to know or access authorization within a security area in order to ensure adherence to security measures,

Security Police Officer (SPO) I: Armed and uniformed Protective Force (PF) officer authorized to carry firearms and make arrests who is employed for, and charged with the protection of classified information and DOE assets and who is required to meet the requirements of 10 CFR Pars 1046 and 1047 and DOE Order 5632.7. Assignments include but are not limited to: Fixed post, no response requirement. This may include access control points, central alarm station, towers, and other monitoring positions.

Security Police Office (SPO) II: An armed and uniformed PF officer authorized to carry firearms and make arrests who is employed for, and charged with the protection of classified information and DOE assets and who is required to meet the requirements of 10 CFR Parts 1046 and 1047 and DOE Order 5632.7. Assignments include but are not limited to: Response positions. This may include alarm response, assessment and containment and patrol duties. Special assignments may include helicopter operations, canine, and vehicle patrol.

Special Police Officer (SPO) III: An armed and uniformed PF officer authorized to carry firearms and make arrests who is employed for, and charged with the protection of classified information and DOE assets and who is required to meet the requirements of 10 CFR Parts 1046 and 1047 and DOE Order 5632.7. Assignments include but are not limited to: Detailed to a special response team as a full time member. SPO III personnel are qualified to perform crisis entry, hostage rescue and other team tactical solutions to adversary activities.

Uniformed Supervisors: Uniformed PF personnel normally holding the rank of: Sergeant, Lieutenant, Captain, Major, Lieutenant Colonel, and Colonel.

### Non-uniformed Support Personnel

Non-uniformed Management and Supervision: Any person whose primary responsibilities include the management or supervision of PF personnel in all areas of work.

Non-uniformed Administration and Clerical: Any person who is primarily responsible for administrative and support tasks that directly support PF personnel and functions.

Logistics Personnel: Any facility security personnel primarily responsible for supply, armory, safety, and maintenance.

Training Personnel: Any personnel whose primary responsibilities include the training of PF.